JUNE 28 - 30, 2005 NORFOLK CONVENTION CENTER

Information Assurance (IA) for FORCEnet (Fn) and Global Information Grid (GIG)

Christopher Newborn

Security Architectures

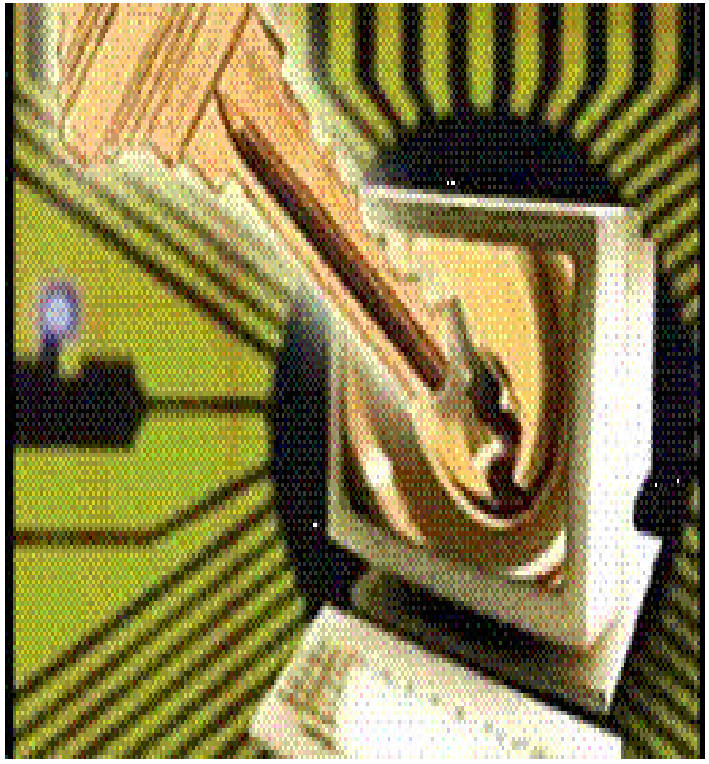
PMW 160/PEO C4I and Space

29 June 2005

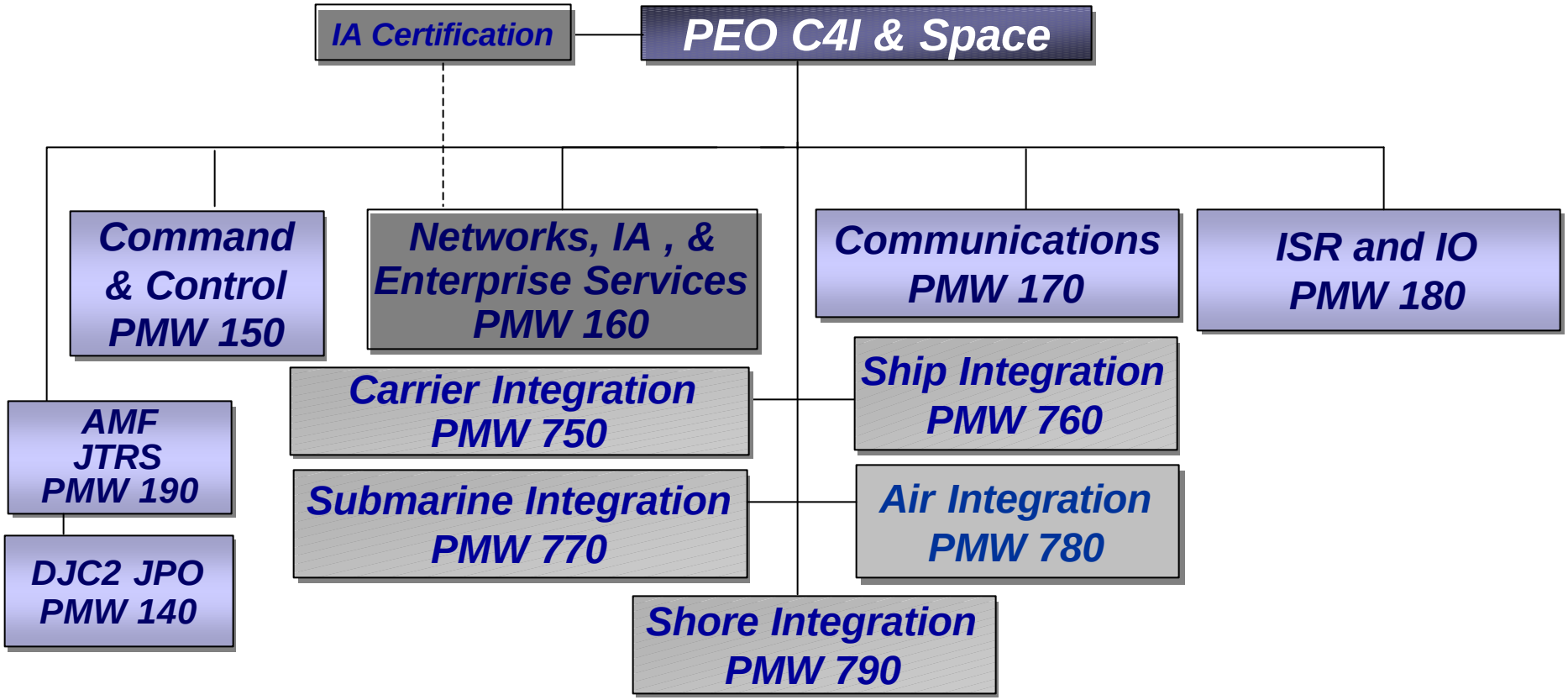
Sponsored by SPAWARSYSCOM FORCEnet Chief Engineer

Agenda

- What is Information Assurance (IA) and why is it important?
- Where is IA going?
- How are we shaping the IA future?
- What are the Issues, Challenges, and Risks?
- What are the Key Takeaways



PEO C4I & Space Organization



Information Assurance is the Enabler for FORCEnet Net-Centricity

PMW 160's IA Charter

- *Captured In OPNAVINST 5239.1B, Navy Information Assurance (IA) Program:*
  - *Serve As Technical Lead for Navy IA*
  - *Provide Systems Security Engineering and Integration Support for All DON Information Systems With IA Requirements*
  - *Budget for DON IA Programs*
  - *Develop and Acquire Standard and Specified IA Products*
  - *Provide Technical Support to Certification Authority (CA)*

Information Protection Evolution

Increasing Net Centricity and Complexity leads to significantly increased risk to the Enterprise

Complexity

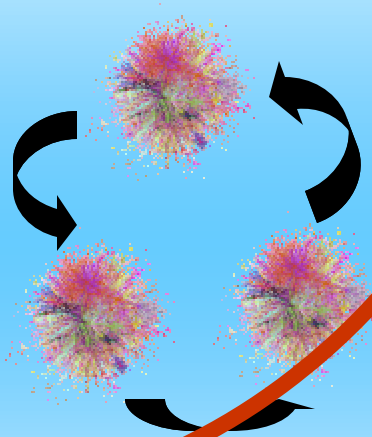
Net Centricity

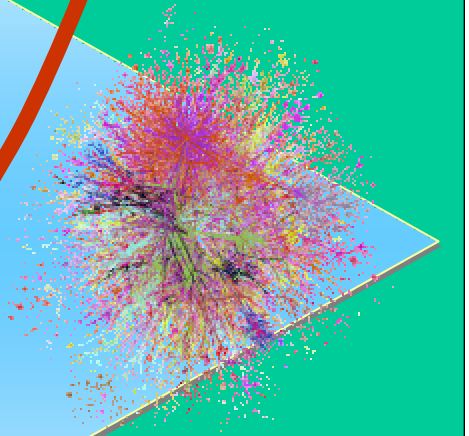
Stovepipe

Point-to-Point

Networked

SOA
(Service Oriented Arch.)





Risk Avoidance

Risk Mitigation

Assured Sharing

What is IA?

"Measures that Protect and Defend Information and Information Systems by Ensuring Their Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. This Includes Providing for Restoration of Information Systems by Incorporating Protection, Detection, and Reaction Capabilities"

Availability	• ***Timely, Reliable Access to Data and Information Services for Authorized Users***
Integrity	• ***Quality of Information System Reflecting Logical Correctness and Reliability of Operating System***
Authentication	• ***Security Measure Designed to Establish Validity of Transmission, Message, or Originator***
Confidentiality	• ***Assurance that Information is Not Disclosed to Unauthorized Entities or Processes***
Non-Repudiation	• ***Assurance Sender of Data is Provided with Proof of Delivery and Recipient with Proof of Sender's Identity***

DoD Directive 8500.1
24 October 2002

Why is IA so Important?

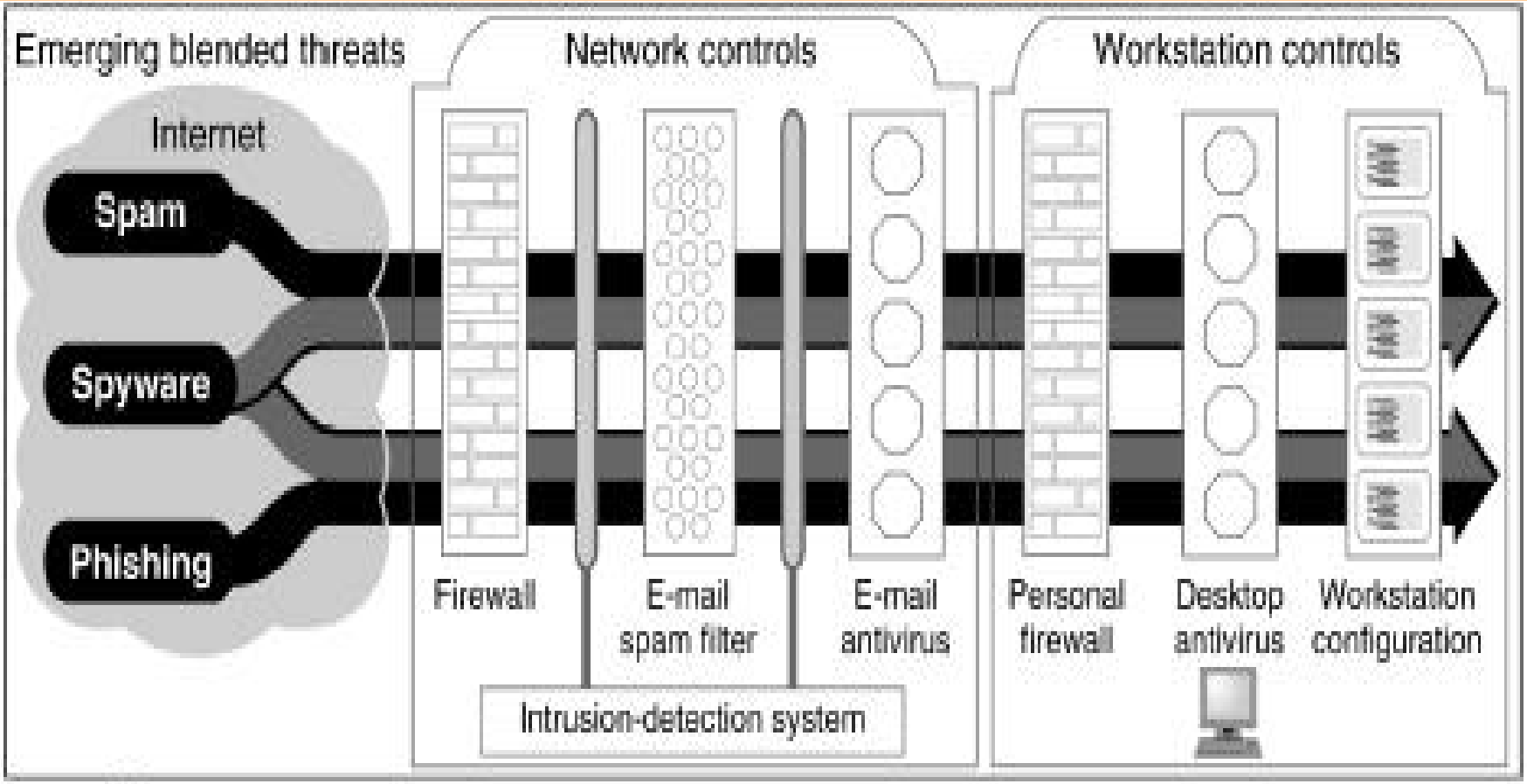
- ***Navy Operates in a Highly Interactive Environment***
  - ***Global Networks***
  - ***Interconnected Applications and Services***
  - ***Powerful Computing Devices***
- ***Components Routinely Interact With***
  - ***Other Services, Governments, Allied/Coalition Partners***
  - ***Other U.S. Government Agencies, Commercial and Research Partners***

The Warfighter must be able to trust their Networks & Data

Complexity of Today's Systems and Networks Presents Significant Security Challenges for Both Producers and Consumers of Information Technology

The Latest Craze

Blending of emerging Cybersecurity Threats can bypass traditional security controls



Source: GAO.

Targets of Opportunity

- The growing number of known vulnerabilities increases the potential number of attacks. Attacks can be launched against specific targets or widely distributed through viruses and worms. Recent examples include:
  - In March 2005, hackers targeted the electric power grid and gained access to electronic control systems
  - In January 2005, a major university reported that a hacker had broken into a database containing 32,000 student and employee Social Security numbers, potentially compromising their finances and identities
  - On August 11, 2003, the Blaster worm was launched, and it infected more than 120,000 computers in its first 36 hours
  - In June 2003, the U.S. government issued a warning concerning a virus that specifically targeted financial institutions
  - In November 2002, a British computer administrator was indicted on charges that he accessed and damaged 98 computers in 14 states between March 2001 and March 2002, causing some $900,000 in damage

Worms/Viruses

- On January 25, 2003, the Slammer worm infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the internet
  - Exploited a known vulnerability for which a patch had been available since July 2002
  - Doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes, causing considerable harm through network outages
  - Even worse if it had carried a malicious payload
  - Unintentionally caused Denial of Service attacks
  - Affected a number of automatic teller machines

Insider Attack

- A system administrator, angered by his diminished role in a thriving defense manufacturing firm, performed the following acts:
  - Centralized the software that supported the company's manufacturing processes on a single server
  - Intimidated a coworker into giving him the only backup tapes for that software
  - Planted a logic bomb on the server
- Following his termination, detonated a logic bomb deleting the only remaining copy of the critical software
- Results: The company estimated the cost of damage in excess of $10 million, which led to the layoff of some 80 employees

***Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors by National Threat Assessment Center United States Secret Service**

What are we doing about it? "INHIBT"

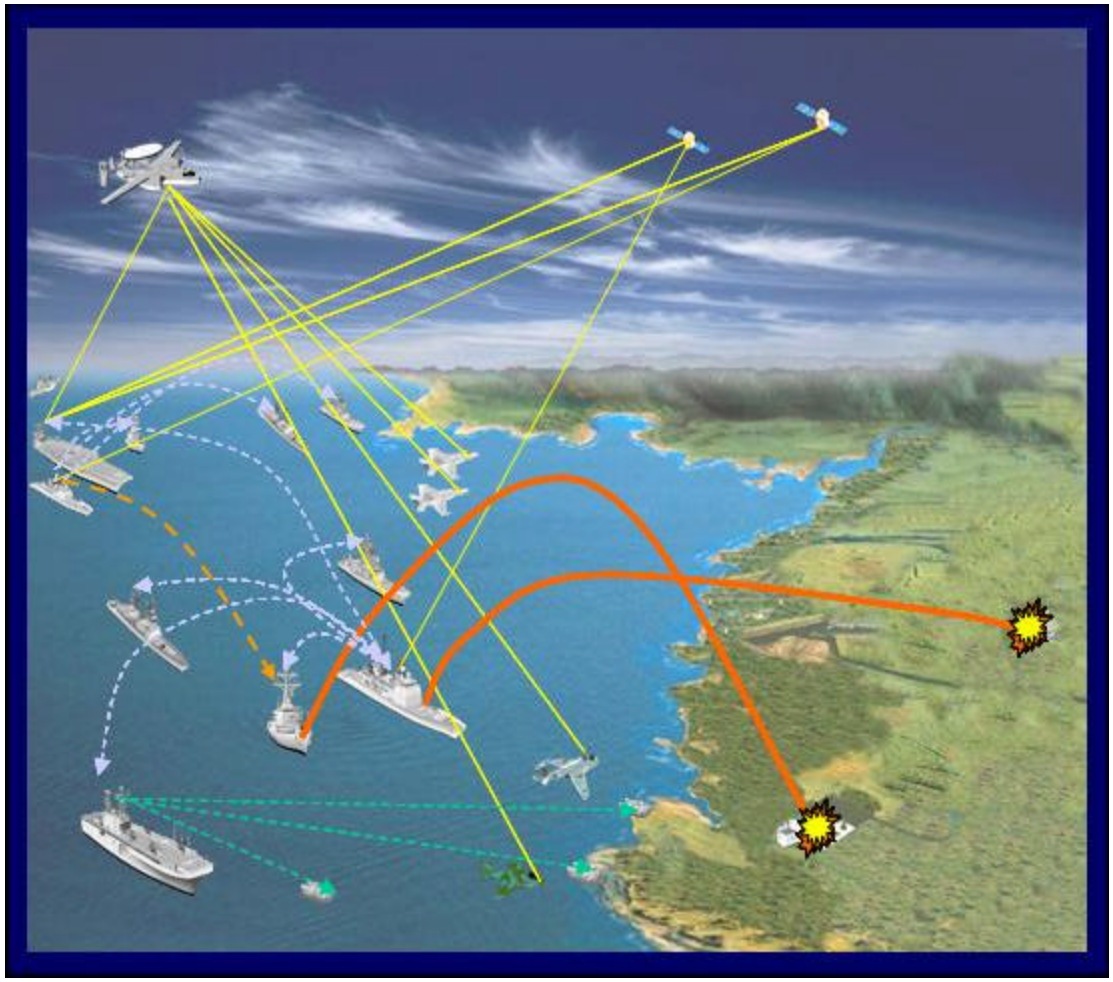
- Set of COTS security products integrated into a holistic architecture.
- Pro-active and reactive, protecting against state-sponsored hackers and the insider threat.
- Protects against malicious code injected by a State-Sponsored agent, insider threat, or amateur hackers.
  - Secure the computers Operating System (O/S)
  - Secure the applications running on your computer
  - Defend against zero-day attacks
  - Non-intrusive to Day-to-Day operations
  - Centrally managed

INHIBT (Independent Host-Based Intrusive Behavior Terminator)

Adversarial Innovation

Core IA Competencies

High Quality IA Products and Services for the Warfighter



Core IA Product Lines

- Network Security Suites
- Cross Domain Solutions
- Cryptographic Products
- Key/Certificate Management
- Secure Voice Technologies
- Biometrics
- Fleet IA Tools (IA Tool Kit)

Core IA Services

- R&D of Emerging Technologies
- Certification and Accreditation
- CNVA and IAVM
- Security Engineering
- TEMPEST Certification
- Education and Awareness
- Naval Publications
- Technical Assistance Services

Where is IA Going?

Crypto

- Reduced Manning Via Software Programmable Multi-Function Crypto Systems That Support Numerous Algorithms and I/O Requirements
- Reduced Footprint and Integration Costs Via Plug and Play Crypto Modules
- Online Management of Self-Aware Crypto Devices Linked To Mission Systems

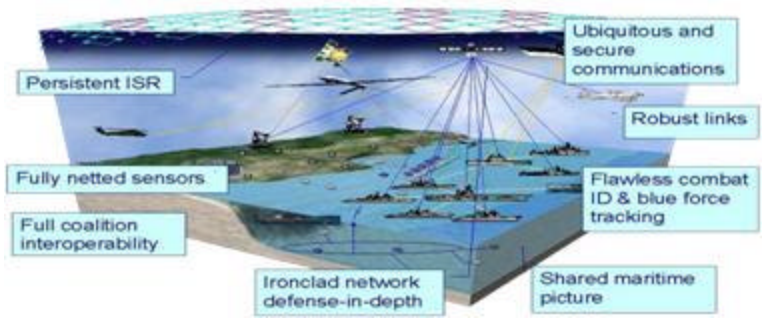
IA Readiness

- On-line Services That Support Minimal Bandwidth Requirements
- IA Vulnerability Management Processes and Technologies That Self-Patch Systems

Key Management Infrastructure

- Secure Distribution and Management of Electronic Key Without "Man in the Loop"

Sea Power 21 With FORCENET



Secure Voice

- Secure Voice Over IP (Type-I)
- End-to-End Secure Communication Channels Regardless of Device or Location

Cross Domain Solutions

- Provide Ubiquitous Joint Allied and Coalition Interoperability

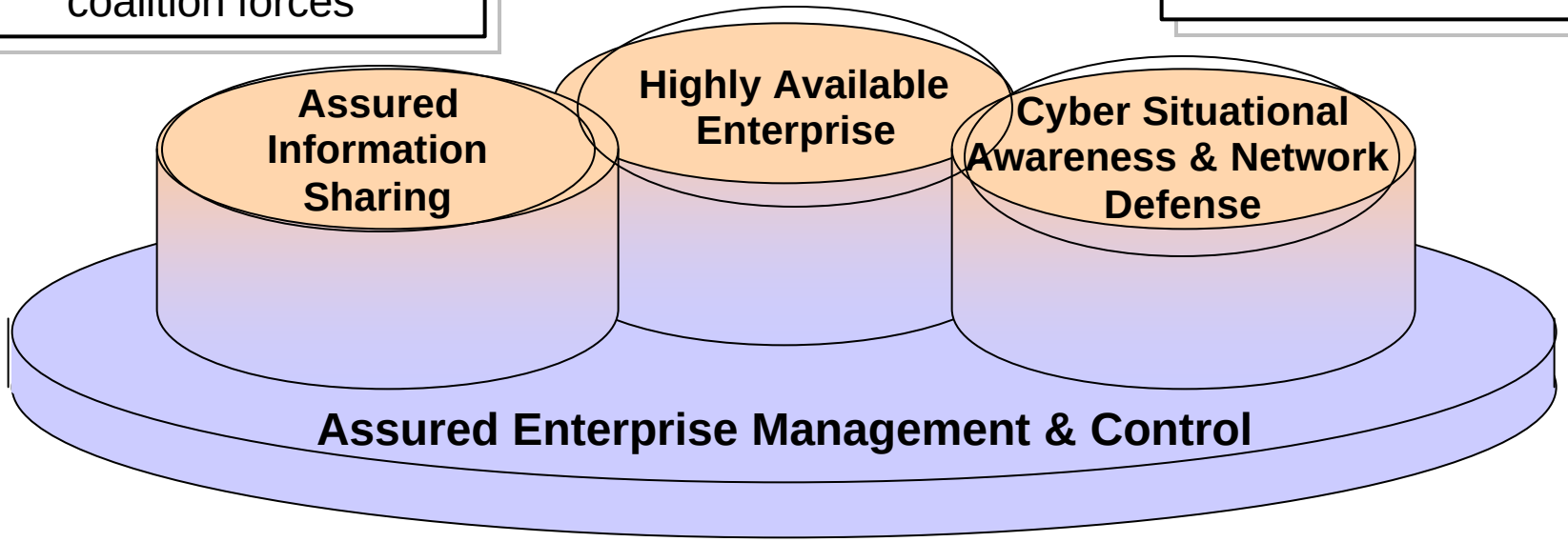
IA is a FORCEnet Enabler

GIG IA Capability Vision 2020

Dynamically and securely **share information** and collaborate at multiple classification levels among U.S., allied and coalition forces

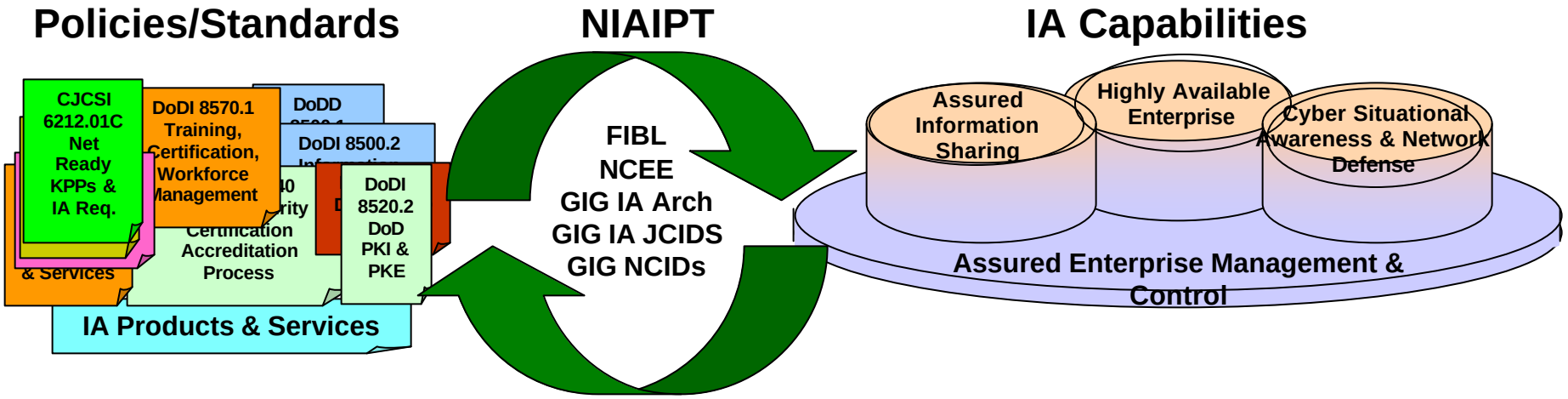
Ensures computing and communications resources, services, and information are **available** to support net-centric operations.

Provides **awareness** of external attacks, insider abuse / misuse. Supports dynamic **adjustment** of security and enterprise resources.



Protects **Management and Control Functions** within each vertical operational area.
Provides common **Security Management Infrastructure** to support all operational areas.

Shaping the IA Future



Does your organization have NIAIPT representation?

Please send POCs information to christopher.newborn@navy.mil

FIBL= FORCEnet Implementation Baseline; NCEE = Naval Collaborative Engineering Environment;
JCIDS = Joint Capabilities Integration & Development System; NCIDs = Netcentric Implementation Documents

Accomplishments

- Assembled NIAIPT membership
  - Need wider Naval participation in the NIAIPT
- Provided a consolidated set of comments for:
  - GIG IA JCIDS (ICD & Supporting Analyses)
  - GIG NCIDs
  - Two Versions of the IA Component of the GIG Arch.
- Responded to OSD/NII regarding the proposed GIG IA Architecture
- GIG IA Implementation Plan
  - Provided data on Naval Access Control, Network structure, bandwidth, and security
  - Informed workgroup on Fn vision, key infrastructure POR's, implementation, etc.
  - Helped define scope and content of the Implementation Plan

Issues and Challenges

- Issues
  - Increased security threats
  - Security is fragmented throughout Navy and DoD; hard to consistently map to GIG and Fn IA requirements
  - Policy and governance is not evolving for an enterprise implementation
- Challenges
  - Increased security threats
  - Develop a Naval IA Security Architecture with standardized products, policies and governance
    - Enforce Configuration Management and penalties for noncompliance
  - Provide well established requirements to developers

Risks

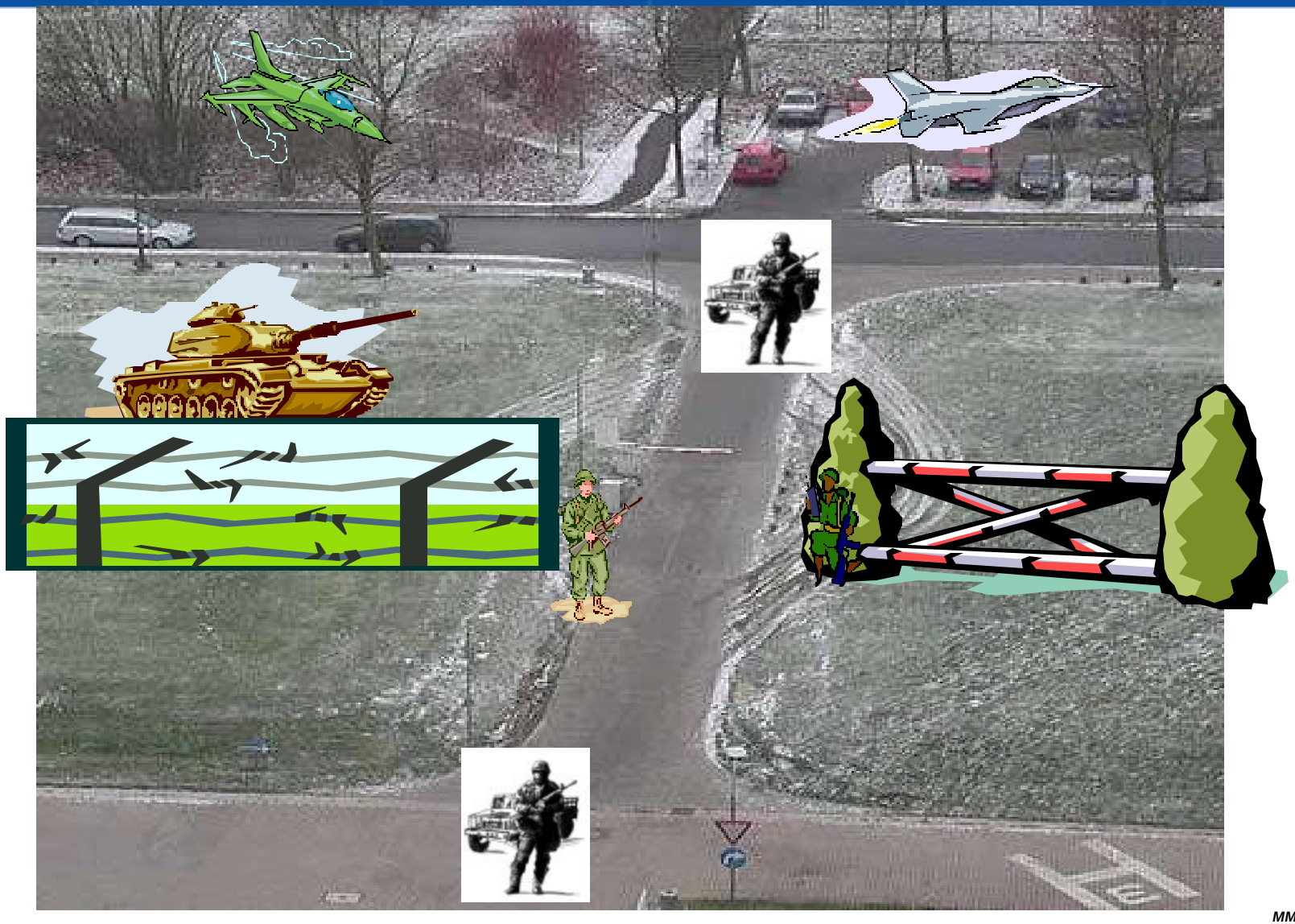
- Risks
  - Increased security threats
  - Reduction or loss of overall enterprise security management
  - Loss of enterprise situation awareness
  - Loss of routing architecture awareness
  - Inability to provide redundant services for NOCs
  - Inability to ensure day-to-day NOC interconnectivity services
    - Authentication, availability, non-repudiation, confidentiality, and integrity

Takeaways

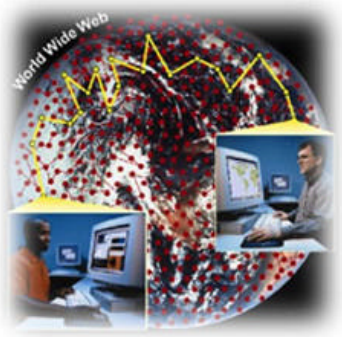
- The Threat is Real
- PMW 160 is engaged in addressing and mitigating the Threat
- Everyone in the DoD community has a responsibility in IA

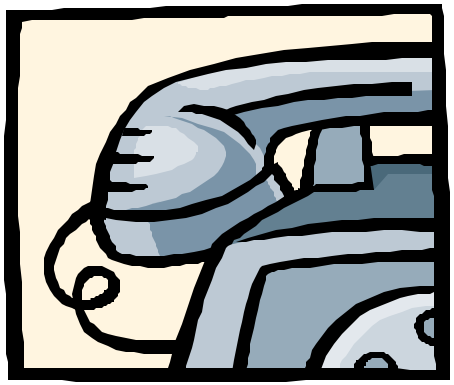
ONLY AS GOOD AS THE WEAKEST LINK

The End Goal



IA





PMW 160

Networks, Information Assurance and Enterprise Services Program Office

robert.wolborsky@navy.mil

DSN 524-7909 / Comm (619) 524-7909

INFOSEC Help Desk: (800) 304-4636

Acronyms

Acronym	Description
ACAT	Acquisition Category
ACC	Alternate Control Center
ACL	Access Control List
ADMS	Automated Digital Multiplexing System
ADNS	Automated Digital Network System
AF	Audio Frequency
AFRL	Air Force Research Laboratory
AMF	Airborne Maritime/Fixed
AMF	Airborne Maritime/Fixed
AMHS	Automated Message Handling System
ANCC	Automated Network Control Center
APM	Assistant Program Manager
ATC	Automated Technical Control
BAN	Base Area Network
BDC	Backup Domain Controller
BIOS	Basic Input Output System
BMV	Bandwidth Managed Voice
BPEL	Business Process Execution Language (for Web Services)
BW	Bandwidth
C&A	Certification and Accreditation
C2PC	Command and Control Personal Computer
C3PO	C4I Common Core Product Overlay
C4I	Command, Control, Communications, Computers and Intelligence
CA	Certification Authority
CAS	Collaboration At Sea
CDD	Capability Development Document
CDF	Channel Definition Format (Microsoft)
CDR	Critical Design Review
CDS	Cross Domain Solutions

Acronyms

CENTCOM	US Central Command
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFE	Customer-Furnished Equipment (contracting)
CFFC	Combined Fleet Forces Command
CFN	Coalition FORCEnet
CJCSI	Chairman Joint Chiefs of Staff Instruction
CJTF	Commander, Joint Task Force
CNO	Chief of Naval Operations
CNVA	Computer Network Vulnerability Assessment
CONET	Coalition Network
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CPD	Capabilities Production Document
CS	Call Server
CSU	Computer Software Unit
CUB	Cryptologic Unified Build
CWSP	Commercial Wideband Satellite-communication Program
DAA	Designated Approving Authority
DATMS-C	DISN (Defense Information System Network) Asynchronous Transfer Mode System
DC	Domain Controller
DIA	Defense Intelligence Agency
DIB	Directory Information Base
DII	Defense Information Infrastructure
DISN	Defense Information Systems Network
DJC2	Deployable Joint Command and Control
DMS	Defense Message System
DNS	Domain Name Server/Service
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction

Acronyms

DON	Department of the Navy
DSA	Directory Service Agent
DSCP	Defense Satellite Communications Program
DSCS	Defense Satellite Communications System
DSN	Digital Switched Network
DSP	Defense Support Program (US DoD satellite system)
DSS	DMS Support Server (Co-Hosted GWS & DSA)
DSU	Data/Digital Service Unit
DSW	DMS Support Workstations (ISNS Workstation w/DSW S/W Load)
DT	Development/al Test/ing
DTW	DoDIIS Trusted Workstation
DWTS	Defense Wide Transmission Systems
EAL	Evaluation Assurance Level
EBEM	Enhanced Bandwidth Efficient Modem
ECP	Engineering Change Proposal
EF	Enterprise Framework
EFW	Embedded Firewall
EHF	Extremely High Frequency (30-300 GHz; 1cm-1mm)
EOC	Early Operational Capability
EPLRS	Enhanced Position Location and Reporting System (also seen as EPLARS)
EUCOM	European Command (USEUCOM)
FAA	Functional Area Analysis
FIBL	FORCEnet Implementation Baseline
Fn	FORCEnet
FNA	Functional Needs Analysis
FOC	Full Operational Capability (DoD acquisition term to depict when a specific activity reaches maturity)
FOT&E	Final Operational Test and Evaluation
FRP	Fleet Response Plan (US Navy)
FSA	Functional Solutions Analysis
FSET	Fleet System Engineering Team

Acronyms

FTP	File Transfer Protocol
FW	Firewall
GCCS-M	Global Command and Control System - Maritime
GCTF	Global Counter-Terrorism Force
GENSER	General Service
GIG	Global Information Grid
GIG-BE	Global Information Grid - Bandwidth Expansion
GIG-ES	Global Information Grid - Enterprise Services
GOTS-D	Government Off-The-Shelf (version Delta)
GUI	Graphical User Interface
GWS	GroupWare Server (DMS/FAMIS applications)
HIDS	Host (based) Intrusion Detection System
HM&E	Hull, Mechanical and Electrical
HTTP	Hypertext Transfer Protocol (world wide web protocol)
HTTPS	Hyper Text Transfer Protocol Secure sockets
IA	Information Assurance
IASM	Intelligent Agent Security Module
IATK	IA Tool Kit
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IBGWN	Intra-Battle Group Wireless Network
IC	Intelligence Community
ICCIO	Intelligence Community Chief Information Officer
ICD	Initial Capabilities Document
IDS	Intrusion Detection System
ILS	Integrated Logistics Support
INE	In-line Network Encryptor
INFOCON	Information Control
INFOSEC	Information Security

Acronyms

INHIBT	Independent Host-Based Intrusive Behavior Terminator
INMARSAT	International Marine/Maritime Satellite
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol
IPD	Integrated Product Development
IPsec	IP Secruity
IPT	Integrated Product Team
IPV6	Internet Protocol Version 6
IRC	Internet Relay Chat
IRP	I/O Request Packet (Microsoft Windows NT)
ISNS	Integrated Shipboard Network System
ISR	Intelligence, Surveillance, and Reconnaissance
ISSM	Information Systems Security Manager
JC2	Joint Command and Control
JCA	Joint Communications Architecture
JCDX	Joint Cross Domain Exchange
JCIDS	Joint Capabilities Integration and Development System
JFCOM	Joint Forces Command
JFN	Joint Fires Network
JIC	Joint Intelligence Center
JOTS	Joint Operational Tactical System
JPO	Joint Program Office
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
KPP	Key Performance Parameter
LCC	Local Control Center
LOS	Line Of Sight (0-30 Miles)
LQOSMAN	Link Quality of Service Manager
LRIP	Low Rate Initial Production

Acronyms

MAGTF	Marine Air-Ground Task Force
MDA	Mail Delivery Agent
MDA	Milestone Decision Authority
METOC	Meteorology and Oceanography
MIDB	Management Information Database
MIS	Management Information Systems
MLS	Multi-Level Security
MLTC	Multi-Level Thin Client
MS	Milestone or Microsoft
MTT	Mobile Training Team
MUX	Multiplex
NAVCIRT	Navy Computer Incident Response Team
NAVMACS	Naval Modular Automated Communications System
NCEE	Naval Collaborative Engineering Environment
NCES	Network Centric Enterprise Services
NCIDs	Net-Centic Implementation Documents
NCTAMS	Naval Computer & Telecommunications Area Master Station
NES	Network Encryption System
NESI	Net-Centric Enterprise Solutions for Interoperability
NETTOP	Network on a Desktop - Virtual Computer
NGA	National Geospatial-Intelligence Agency (formerly National Imagery and Mapping Agency)
NIAIPT	Naval Information Assurance Integrated Product Team
NIC	Network Interface Card (PC Ethernet network card)
NIDS	Network Intrusion Detection Systems
NIDTS	NATO Initial Data Transfer System
NIF	Network Intrusion Filter
NII	Networks and Integrated Information
NIPRNET	Non-Classified Internet Protocol Router Network (US DoD)
NNWC	Naval Network Warfare Command
NOC	Network Operations Center

Acronyms

NREMS	Navy Regional Enterprise Messaging System
NRO	National Reconnaissance Office
NSA	National Security Agency
NSGA	Naval Security Group Activity
NTCSS	Navy Tactical Command Support System
NTDPS	Non-Tactical Data Processing Sub-system
OASD	Office of the Assistant Secretary of Defense
OCSP	Online Certificate Status Protocol
OED	OSIS Evolutionary Development
ONE-NET	OCONUS Navy Enterprise Network (formerly Base Level Information Infrastructure (BLII)
OS or O/S	Operating System
OSIS	Ocean Surveillance Information System
OSPF	Open Shortest Path First
OT	Operational Test/ing
OWFIT	One Way File Transfer
PACOM	Pacific Command (USPACOM)f
PBR	Policy Based Routing
PDR	Preliminary Design Review
PDU	Packet Data Unit
PEO	Program Executive Office
PKE	Public Key Encryption/Equipment
PKI	Public Key Infrastructure
PMW	Program Manager Warfare
POC	Point Of Contact
POC	Point of Contact
POR	Program of Record
POTS	Plain Old Telephone System
PPL	Preferred Products List
QOS	Quality Of Service
R&D	Research & Development

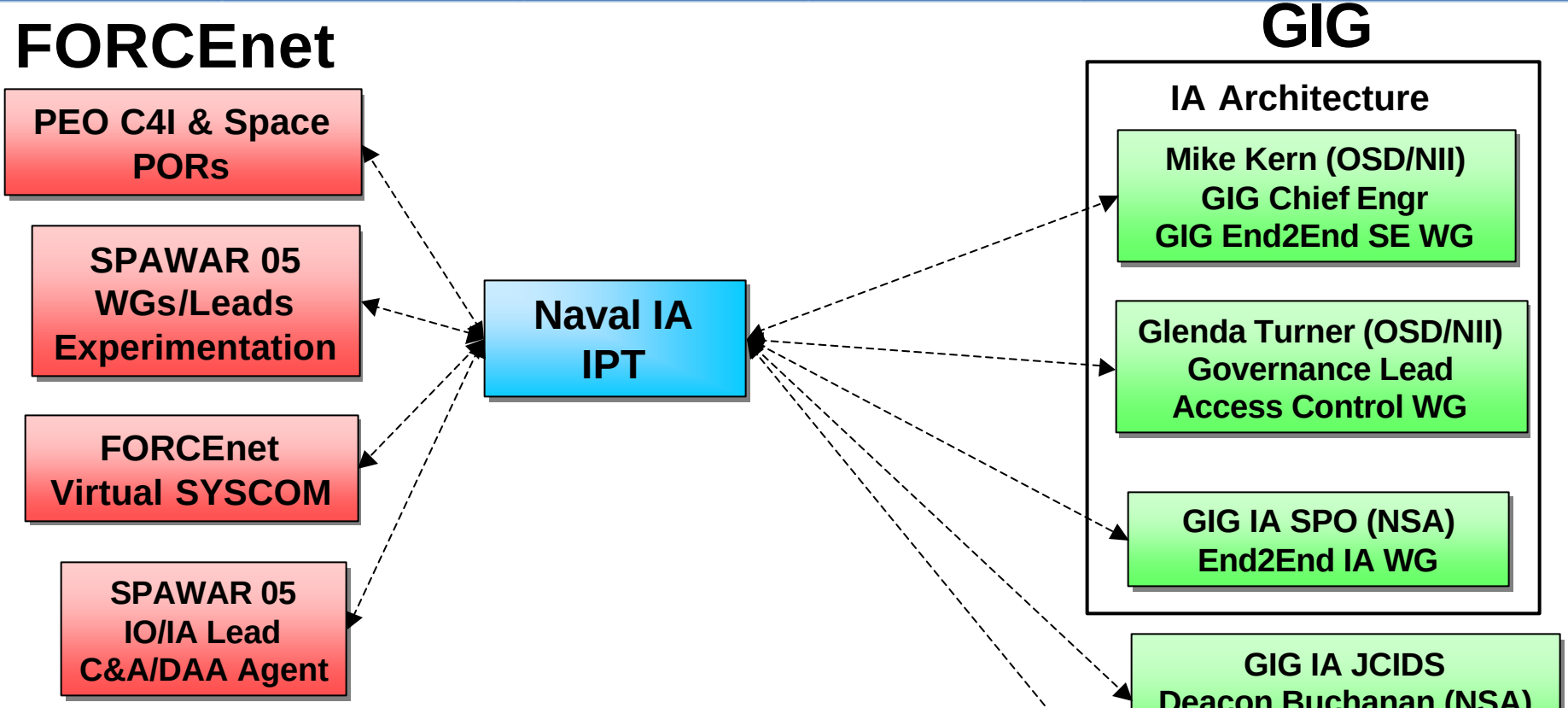
Acronyms

RAS	Remote Access Service
RF	Radio Frequency
RFC	Required Functional Capability
RFI	Request For Information
RPC	Remote Procedure Call
RTR	Router
S&T	Science & Technology
SAP	Systems, Applications & Products in Data Processing
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SCA	Single-Connector Attachment (SCSI)
SCD	Ship Change Document
SCI	Sensitive Compartmented Information
SCSI	Small Computer System Interface
SE	Systems Engineering
SELINUX	Security Enhanced Linux
SHF	Super High Frequency (3-30 GHz; 10-1cm)
SI	Special Intelligence
SINCGARS	Single Channel Ground to Air Radio System
SIP	Serial Interface Protocol
SIPRNET	Secret Internet Protocol Router Network
SMS	Single Messaging Solution
SMTP	Simple Mail Transfer Protocol (internet email)
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol (XML protocol)
SPO	Special Program Office
SSEE	Ships Signal Exploitation Equipment
SSL	Secure Sockets Layer (Netscape; web security protocol)
STRATCOM	US Strategic Command
SWT	Switch

Acronyms

SYSCOM	Systems Command
TACLANE	Tactical Local Area Network Encryptor
TBMCS	Theater Battle Management Control System
TC	Transformational Communications
TCP	Transmission Control Protocol (with Internet Protocol [IP], the main protocol of the Internet)
TDAMS	Tactical Decision Aid Monitoring System
TDM	Time Division Multiplexer/Multiplexing
TIP	TDMA (Time Division Multiplex Access) Interface Processor
TRE	Tactical Receive Equipment
TSAT	Transformational Communications Satellite
TSE	Tactical Support Element/Equipment
TW	Trident Warrior (exercise name)
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USMC	United States Marine Corps
VM	Virtual Machine
VMM	Virtual Machine Module
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSCAN	Virus Scan
VTCOIP	Video Teleconferencing over Internet Protocol
WAN	Wide Area Network
WEBDAV	Web-Based Distributed Authoring and Versioning (HTTP extensions)
WNW	Wideband Network Waveform (new for Joint Tactical Radio System program)
WRT	With Respect To
XML	eXtensible Markup Language

NIAIPT Focus Groups



Engaged to make Fn/GIG IA a reality for the Naval Services